PCT/JP2004/017453

日本国特許庁
JAPAN PATENT OFFICE

02.12.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

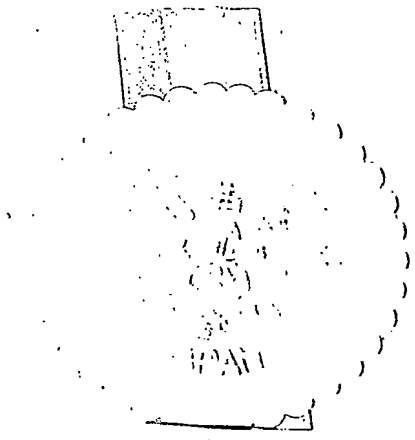
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１１月２８日

出願番号
Application Number: 特願２００３－３９９９６８

[ST. 10/C]: [ＪＰ２００３－３９９９６８]

出願人
Applicant(s): 松下電器産業株式会社



２００５年 １月１３日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号 出証特２００４－３１２２１４９

【書類名】　特許願
【整理番号】　2048150054
【提出日】　平成15年11月28日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【発明者】
　【住所又は居所】　東京都江東区青梅２－７９　東京国際交流館Ａ０９０９
　【氏名】　ナッタポン　アッタラパドゥン
【発明者】
　【住所又は居所】　東京都三鷹市大沢２－２０－３１－１－４０２
　【氏名】　古原　和邦
【発明者】
　【住所又は居所】　神奈川県横浜市戸塚品濃町５５７－４４－２０５
　【氏名】　今井　秀樹
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742

【書類名】特許請求の範囲
【請求項１】
特定の装置を無効化するための無効化情報の生成を行い配布する鍵管理装置と、前記無効化情報を記録する記録媒体と、前記記録媒体から前記無効化情報を読み出して処理する端末装置からなる著作権保護システムであって、
前記鍵管理装置は、
前記著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、
前記部分集合に対して鍵を割り当てる割当部と、
前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、
前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備えることを特徴とする著作権保護システム。
【請求項２】
前記鍵管理装置の鍵生成部は、前記部分集合に割り当てられた鍵から、一方向性関数を利用して他の部分集合の鍵を生成することを特徴とする請求項１記載の著作権保護システム。
【請求項３】
前記鍵管理装置の鍵生成部は、前記部分集合に割り当てられた鍵から、複数の他の部分集合の鍵を生成することを特徴とする請求項１記載の著作権保護システム。
【請求項４】
前記鍵管理装置はさらに、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を記憶する記憶部を備えることを特徴とする請求項１記載の著作権保護システム。
【請求項５】
前記鍵管理装置の記憶部は、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を、テーブルを利用して管理し、前期テーブルを記憶することを特徴とする請求４記載の著作権保護システム。
【請求項６】
前記鍵管理装置はさらに、前記部分集合に対して割り当てた鍵を前記端末装置に配布する鍵配布部を備え、
前記鍵配布部は、鍵を配布する端末装置が含まれる部分集合のうち、最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布し、さらに、前記配布した鍵から生成される鍵が割り当てられた部分集合を除く部分集合から、前記端末装置が含まれる最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布することを特徴とする請求項１記載の著作権保護システム。
【請求項７】
前記鍵管理装置の無効化情報生成部は、有効な端末装置だけが含まれる最大の部分集合を選択して、前記選択した部分集合に含まれない端末装置に対しては、さらに、それら端末装置だけが含まれる最大の部分集合を選択して、前記選択を、全ての有効な端末装置が何れかの部分集合に含まれるまで繰り返し行うことを特徴とする請求項１記載の著作権保護システム。
【請求項８】
前記端末装置はさらに、前記無効化情報を処理する鍵を格納する格納部を備え、
前記格納部には、自身が含まれる部分集合に割り当てられた鍵を格納することを特徴とする請求項１記載の著作権保護システム。
【請求項９】
前記端末装置の格納部は、鍵と部分集合の対応関係を示す情報も合わせて格納することを特徴とする請求項８記載の著作権保護システム。
【請求項１０】
前記端末装置の格納部は、ある部分集合に割り当てられた鍵から、他の部分集合の鍵が

生成可能な場合、前記生成可能な鍵は格納しないことを特徴とする請求項８記載の著作権保護システム。

【請求項１１】

前記端末装置はさらに、前記格納部に格納する鍵から、他の部分集合に割り当てられた鍵を生成する鍵生成部を備え、

前記鍵生成部は、部分集合と鍵の対応関係、並びに生成された鍵の相互関係から他の部分集合に割り当てられた鍵を生成することを特徴とする請求項１０記載の著作権保護システム。

【請求項１２】

前記端末装置はさらに、前記記録媒体に対して、暗号化されたコンテンツを記録する記録部を備えることを特徴とする請求項１記載の著作権保護システム。

【請求項１３】

前記端末装置はさらに、前記記録媒体から暗号化されたコンテンツを読み出して復号、及び再生する再生部を備えることを特徴とする請求項１記載の著作権保護システム。

【請求項１４】

前記鍵管理装置が生成した無効化情報には、どの部分集合の鍵に基づいて生成したのかを示す情報が付与されることを特徴とする請求項１記載の著作権保護システム。

【請求項１５】

前記記録媒体の代わりに通信媒体を利用することを特徴とする請求項１記載の著作権保護システム。

【請求項１６】

特定の装置を無効化するための無効化情報の生成を行い配布する鍵管理装置であって、

前記鍵管理装置は、

前記著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、

前記部分集合に対して鍵を割り当てる割当部と、

前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、

前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備えることを特徴とする鍵管理装置。

【請求項１７】

前記鍵生成部は、前記部分集合に割り当てられた鍵から、一方向性関数を利用して他の部分集合の鍵を生成することを特徴とする請求項１６記載の鍵管理装置。

【請求項１８】

前記鍵生成部は、前記部分集合に割り当てられた鍵から、複数の他の部分集合の鍵を生成することを特徴とする請求項１６記載の鍵管理装置。

【請求項１９】

前記鍵管理装置はさらに、

前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を記憶する記憶部を備えることを特徴とする請求項１６記載の鍵管理装置。

【請求項２０】

前記記憶部は、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を、テーブルを利用して管理し、前期テーブルを記憶することを特徴とする請求１９記載の鍵管理装置。

【請求項２１】

前記鍵管理装置はさらに、前記部分集合に対して割り当てた鍵を前記端末装置に配布する鍵配布部を備え、

前記鍵配布部は、鍵を配布する端末装置が含まれる部分集合のうち、最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布し、さらに、前記配布した鍵から生成される鍵が割り当てられた部分集合を除く部分集合から、前記端末装置が含まれる最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布すること

を特徴とする請求項１６記載の鍵管理装置。
【請求項２２】
前記無効化情報生成部は、有効な端末装置だけが含まれる最大の部分集合を選択して、前記選択した部分集合に含まれない端末装置に対しては、さらに、それら端末装置だけが含まれる最大の部分集合を選択して、前記選択を、全ての有効な端末装置が何れかの部分集合に含まれるまで繰り返し行うことを特徴とする請求項１６記載の鍵管理装置。
【請求項２３】
記録媒体から無効化情報を読み出して処理する端末装置であって、
前記端末装置は、前記無効化情報を処理する鍵を格納する格納部を備え、
前記格納部には、自身が含まれる部分集合に割り当てられた鍵を格納することを特徴とする端末装置。
【請求項２４】
前記格納部は、鍵と部分集合の対応関係を示す情報も合わせて格納することを特徴とする請求項２３記載の端末装置。
【請求項２５】
前記格納部は、ある部分集合に割り当てられた鍵から、他の部分集合の鍵が生成可能な場合、前記生成可能な鍵は格納しないことを特徴とする請求項２３記載の端末装置。
【請求項２６】
前記端末装置はさらに、前記格納部に格納する鍵から、他の部分集合に割り当てられた鍵を生成する鍵生成部を備え、
前記鍵生成部は、部分集合と鍵の対応関係、並びに生成された鍵の相互関係から他の部分集合に割り当てられた鍵を生成することを特徴とする請求項２５記載の端末装置。
【請求項２７】
前記端末装置はさらに、前記記録媒体に対して、暗号化されたコンテンツを記録する記録部を備えることを特徴とする請求項２３記載の端末装置。
【請求項２８】
前記端末装置はさらに、前記記録媒体から暗号化されたコンテンツを読み出して復号、及び再生する再生部を備えることを特徴とする請求項２３記載の端末装置。
【請求項２９】
特定の装置を無効化するための無効化情報を記録する記録媒体であって、
鍵管理装置は、著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備え、
前記鍵管理装置により生成された無効化情報を記録することを特徴とする記録媒体。
【請求項３０】
前記鍵管理装置が生成した無効化情報には、どの部分集合の鍵に基づいて生成したのかを示す情報が付与されており、前記付与された情報と共に前記鍵無効化情報を記録することを特徴とする請求項２９記載の記録媒体。

【書類名】明細書
【発明の名称】著作権保護システム、鍵管理装置、端末装置、及び記録媒体
【技術分野】
【０００１】
本発明は、映画や音楽などの著作物であるコンテンツのデジタル化データを、光ディスク等の大容量記録媒体に記録、あるいは再生するシステムに関し、特に不正装置を使ったコンテンツの記録、あるいは再生による著作権侵害を防止するために、不正装置が持つ鍵では、コンテンツの記録、あるいは再生に必要な鍵が算出できず、不正装置以外の正規装置では、いずれの装置においても共通の鍵が算出できるような著作権保護システムに関する。
【背景技術】
【０００２】
近年、マルチメディア関連技術の発展、大容量記録媒体の出現等を背景として、動画、音声等からなるデジタルコンテンツ（以下、コンテンツ）を生成して、光ディスク等の大容量記録媒体に格納して配布する、あるいはネットワークや放送を介して配信するシステムが現れている。
配信されたコンテンツは、コンピュータや再生装置等で読み出されて、再生、あるいはコピーの対象となる。
【０００３】
一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピーといった不正利用を防止するために暗号化技術が用いられる。
具体的には、コンテンツをある暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号化鍵に対応する復号鍵を保有する端末のみが、記録媒体から読み出したデータをその復号鍵を用いて復号して、コンテンツの再生等を行うことができる、というものである。なお、コンテンツを暗号化して記録媒体に記録する方法としては、端末が保有する復号鍵に対応する暗号化鍵でコンテンツそのものを暗号化して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、端末が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法等がある。
【０００４】
このとき、端末が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による端末内部の解析において、ある鍵が外部に暴露される危険性がある。ある鍵が一旦不正者に暴露されてしまうと、コンテンツを不正利用する記録装置、再生装置、あるいはソフトウェアを作成し、インターネット等によりそれらを流布することが考えられる。このような場合、著作権者は一旦暴露された鍵では、次から提供するコンテンツを扱えないようにしたいと考える。これを鍵無効化技術と呼び、鍵無効化を実現するシステムとして、木構造と呼ばれる階層構造を利用した鍵無効化技術が、特許文献１、及び非特許文献１に開示されている。
【０００５】
以下、非特許文献１に記載されている従来の鍵無効化技術について説明する。
まず、「Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ」（以降、差分集合と呼ぶ）についての定義を行う。差分集合は、大きな木構造の集合から、それよりも小さな木構造の集合を取り除いたときの、各装置（リーフ）からなる集合と定義する。大きな木構造のルートと小さな木構造のルートの２つを定めることにより、差分集合は決定される。そして、各差分集合に対してそれぞれ復号鍵が割り当てられる。
【０００６】
さらに、コンテンツはコンテンツ鍵で暗号化されており、各装置は復号鍵を保持し、各装置が自身の保持する復号鍵を用いてコンテンツ鍵を求める際に必要とされるデータを鍵データと呼ぶ。一般的に、鍵データはコンテンツ共に配信され、コンテンツの配信に記録媒体を利用する場合は、鍵データは記録媒体に記録される。

無効化されない装置の集合を、差分集合でカバーすることによって、鍵データのサイズを削減することが可能となる。図１５にその概念図を示す。図１５において、大きな木構造のルートをＶｉ、小さな木構造のルートをＶｊとした場合、印をつけた２つのリーフに割り当てられた装置を無効化する集合は、ＶｉをルートとするＶｊをルートとする木構造を取り除いた差分集合Ｓｉ，ｊとなる。さらに、必要となる鍵データは、前記差分集合Ｓｉ，ｊに対応した１つの暗号化鍵Ｌｉ，ｊを用いて暗号化された、１つの暗号化コンテンツ鍵となる。

【０００７】

また、別の例として、装置数１６の木構造において、装置３、装置４、装置１３、装置１５が無効化されている場合の差分集合、並びにコンテンツ鍵を暗号化するための暗号化鍵Ｓｉ，ｊを図１６に示す。例えば、装置９～装置１２は、Ｖ３をルートとする木構造から、Ｖ７をルートとする木構造を取り除いた差分集合Ｓ３，７に属する。図１６おいては、同一の差分集合Ｓｉ，ｊに属する装置は、共通の復号鍵を保持している。例えば、差分集合Ｓ２，９に属する装置１、装置２、装置５～装置８は、共通の復号鍵Ｌ２，９を保持し、差分集合Ｓ３，７に属する装置９～装置１２は、共通の復号鍵Ｌ３，７を保持している。さらに、コンテンツ鍵は、Ｌ２，９、Ｌ３，７、Ｌ１４，２８、Ｌ１５，３１でそれぞれ暗号化されるため、いずれの復号鍵も保持していない装置３、装置４、装置１３、装置１５は、コンテンツ鍵を復号することができず、コンテンツを扱うことができない。

【０００８】

ここで、各装置は、無効化される装置の位置関係に応じた復号鍵を保持する必要があり、その基本的な考え方は次の通りである。ある装置が差分集合Ｓｉ，ｊに対応した復号鍵Ｌｉ，ｊを保持する場合、その装置は、差分集合Ｓｉ，ｋに対応した復号鍵Ｌｉ，ｋも保持する。ただし、ＶｋはＶｊの部分集合とする。このとき、Ｌｉ，ｋは、Ｌｉ，ｊから計算で求めることができるようにするが、その逆は計算では求められないようにするため一方向性関数を利用する。

【０００９】

まず、木構造の各ノードに割り当てられる暗号化鍵（この暗号化鍵は、各装置が保持する復号鍵と対応する）について、図１７に示す２分木の木構造の例を用いて説明する。

図１７に示す木構造の各ノードには、それぞれ個別のＴビットの「ラベル」と呼ばれる識別子が付与されている。そして、入力データ長Ｔビットに対して、３Ｔビットの乱数を生成する擬似乱数生成器Ｇを用意する。ラベルＡ１を擬似乱数生成器Ｇの入力とした場合に、出力される３Ｔビットのうち、前半Ｔビットをラベル Ａ１の左下の子のラベルとし、真ん中のＴビットをラベルＡ１のノードに対応する暗号化鍵とし、後半Ｔビットをラベル Ａ１の右下の子のラベルとし、それぞれをＡ１Ｌ、Ａ１Ｍ、Ａ１Ｒと表現する。図１７では、各ノードには予めラベルＡ１、Ａ２、Ａ３、Ａ４等が個別に割り当てられており、加えて上位のラベルから派生してきた新たなラベルが追加される。例えば、上から３層目のノード４００１においては、当該ノードに予め割り当てられたラベルＡ４に加え、上位のラベルＡ１から派生したラベルＡ１ＬＬ、並びに同じく上位のラベルＡ２から派生したラベルＡ２Ｌと計３個のラベルが割り当てられことになる。さらに、各ノードに割り当てられる暗号化鍵の数は、当該ノードに割り当てられたラベルの数と等しくなるため、ノード４００１には、Ａ１ＬＬＭ、Ａ２ＬＭ、Ａ４Ｍの計３つの暗号化鍵が割り当てられることになる。

【００１０】

ここで、差分集合Ｓｉ，ｊに対応する暗号化鍵Ｌｉ，ｊと、上記各ノードに割り当てられた暗号化鍵の関係を示す。ノードＶｉとノードＶｊを決定した場合、差分集合Ｓｉ，ｊに対応する暗号化鍵Ｌｉ，ｊは、ノードＶｉに割り当てられたラベルから派生したラベルのうち、ノードＶｊに追加されたラベルに対応する暗号化鍵となる。図１７の例において、ノードＶｉのラベルをＡ１、ノードＶｊのラベルをＡ４とすると、暗号化鍵Ｌｉ，ｊはＡ１ＬＬＭとなる。

【００１１】

次に、各装置に割り当てる復号鍵について説明する。ここでは、各装置には、ノードに割り当てられる複数のラベルが割り当てられるものとし、各装置は、装置内で、対応するラベルと擬似乱数生成器Ｇから復号鍵を生成するものとする。さらに、暗号化鍵と復号鍵が等しい秘密鍵暗号をその一例として説明する。

具体的には、各装置が割り当てられたリーフから、ルートに至る経路上に存在するノードにぶら下がるノードに着目して、当該ノードに割り当てられているラベルが、各装置に対して割り当てられる。その具体例を図１８に示す。

【００１２】

図１８は、装置の総数を８台としたときの、各装置に割り当てられるラベルを示している。装置１に割り当てられるラベルは、装置１からルートに至る経路上に存在するノードＡ、ノードＢ、ノードＤにそれぞれぶら下がるノードＣ、ノードＥ、及び装置２が割り当てられるリーフのラベルである。図１８に示す通り、各装置に対しては該当するラベルが全て割り当てられる。このとき、各装置に割り当てられるラベルの総数は、装置の総数をｔ台とした場合、$0.5(\log_2 t)^2+0.5\log_2 t$個である。これは、各装置に割り当てられるラベルの数が、２層目に１個、３層目に２個、…、最下位層に$\log_2 t$個であることから、$1+2+\cdots+\log_2 t=0.5(\log_2 t)^2+0.5\log_2 t$となるからである。

【００１３】

次に、図１８を用いて、実際に装置を無効化する場合の例を説明する。

（１）何れの装置も無効化されていない初期状態では、ラベルＡＬ、ＡＲに対応する鍵ＡＬＭ、及びＡＲＭを用いてコンテンツ鍵を暗号化する。全ての装置は、ラベルＡＬ、あるいはラベルＡＲを保持しており、それらから、復号鍵ＡＬＭ、あるいはＡＲＭを生成することができる。従って、生成した復号鍵でコンテンツ鍵を復号することができ、さらには、復号したコンテンツ鍵を利用してコンテンツを復号することができる。

【００１４】

（２）装置１がハックされて、保持する全ての鍵が暴露された場合は、ラベルＡとラベルＡＬＬＬを指定して、ラベルＡをルートとする大きな木構造から、ラベルＡＬＬＬの小さいな木構造（リーフ）を取り除く。そして、ラベルＡＬＬＬに対応する暗号化鍵ＡＬＬＬＭを用いてコンテンツ鍵を暗号化する。装置２は、ラベルＡＬＬＬから復号鍵ＡＬＬＬＭを生成することができ、装置３、装置４は、ラベルＡＬＬから復号鍵ＡＬＬＬＭを生成することができ、さらに、装置５～装置８は、ラベルＡＬから復号鍵ＡＬＬＬＭを生成することができる。装置１は、擬似乱数生成器Ｇが一方向性であることから、自身が保持するラベルからは復号鍵ＡＬＬＬＭを生成することができないため、コンテンツ鍵を復号することができない。

【００１５】

最後に、非特許文献１に示す従来の鍵無効化技術においては、装置数が約１０億台（高さ３０の２分木）のシステムを考えた場合、各装置が保持する鍵の数は４６５個となる。

【特許文献１】特開２００２－２８１０１３号公報

【非特許文献１】D. Naor, M. Naor, and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers", Proceedings of CRYPTO2001, LNCS2139, pp.41-62, 2001.

【発明の開示】

【発明が解決しようとする課題】

【００１６】

しかしながら、非特許文献１に開示されている従来の鍵無効化技術では、各装置が内蔵する鍵の数が膨大になるという課題がある。

本発明は、前記従来の課題を解決するためのもので、各装置が内蔵する鍵の数を削減可能な鍵無効化システムの提供を目的とする。

【課題を解決するための手段】

【００１７】

本発明は、特定の装置を無効化するための無効化情報の生成を行い配布する鍵管理装置

と、前記無効化情報を記録する記録媒体と、前記記録媒体から前記無効化情報を読み出して処理する端末装置からなる著作権保護システムであって、前記鍵管理装置は、前記著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備えることを特徴とする。

【００１８】

また、本発明は、前記著作権保護システムであって、前記鍵管理装置の鍵生成部は、前記部分集合に割り当てられた鍵から、一方向性関数を利用して他の部分集合の鍵を生成することを特徴とする。

また、本発明は、前記著作権保護システムであって、前記鍵管理装置の鍵生成部は、前記部分集合に割り当てられた鍵から、複数の他の部分集合の鍵を生成することを特徴とする。

【００１９】

また、本発明は、前記著作権保護システムであって、前記鍵管理装置は、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を記憶する記憶部を備えることを特徴とする。

また、本発明は、前記著作権保護システムであって、前記鍵管理装置の記憶部は、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を、テーブルを利用して管理し、前期テーブルを記憶することを特徴とする。

【００２０】

また、本発明は、前記著作権保護システムであって、前記鍵管理装置は、前記部分集合に対して割り当てた鍵を前記端末装置に配布する鍵配布部を備え、前記鍵配布部は、鍵を配布する端末装置が含まれる部分集合のうち、最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布し、さらに、前記配布した鍵から生成される鍵が割り当てられた部分集合を除く部分集合から、前記端末装置が含まれる最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布することを特徴とする。

【００２１】

また、本発明は、前記著作権保護システムであって、前記鍵管理装置の無効化情報生成部は、有効な端末装置だけが含まれる最大の部分集合を選択して、前記選択した部分集合に含まれない端末装置に対しては、さらに、それら端末装置だけが含まれる最大の部分集合を選択して、前記選択を、全ての有効な端末装置が何れかの部分集合に含まれるまで繰り返し行うことを特徴とする。

【００２２】

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記無効化情報を処理する鍵を格納する格納部を備え、前記格納部には、自身が含まれる部分集合に割り当てられた鍵を格納することを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置の格納部は、鍵と部分集合の対応関係を示す情報も合わせて格納することを特徴とする。

【００２３】

また、本発明は、前記著作権保護システムであって、前記端末装置の格納部は、ある部分集合に割り当てられた鍵から、他の部分集合の鍵が生成可能な場合、前記生成可能な鍵は格納しないことを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記格納部に格納する鍵から、他の部分集合に割り当てられた鍵を生成する鍵生成部を備え、前記鍵生成部は、部分集合と鍵の対応関係、並びに生成された鍵の相互関係から他の部分集合に割り当てられた鍵を生成することを特徴とする。

【００２４】

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記記録媒体に対して、暗号化されたコンテンツを記録する記録部を備えることを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記記録媒体から暗号化されたコンテンツを読み出して復号、及び再生する再生部を備えることを特徴とする。

【００２５】

また、本発明は、前記著作権保護システムであって、前記鍵管理装置が生成した無効化情報には、どの部分集合の鍵に基づいて生成したのかを示す情報が付与されることを特徴とする。

また、本発明は、前記著作権保護システムであって、前記記録媒体の代わりに通信媒体を利用することを特徴とする。

【００２６】

また、本発明は、特定の装置を無効化するための無効化情報の生成を行い配布する鍵管理装置であって、前記鍵管理装置は、前記著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備えることを特徴とする。

【００２７】

また、本発明は、前記鍵管理装置であって、前記鍵生成部は、前記部分集合に割り当てられた鍵から、一方向性関数を利用して他の部分集合の鍵を生成することを特徴とする。

また、本発明は、前記鍵管理装置であって、前記鍵生成部は、前記部分集合に割り当てられた鍵から、複数の他の部分集合の鍵を生成することを特徴とする。

また、本発明は、前記鍵管理装置であって、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を記憶する記憶部を備えることを特徴とする。

【００２８】

また、本発明は、前記鍵管理装置であって、前記記憶部は、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を、テーブルを利用して管理し、前期テーブルを記憶することを特徴とする。

また、本発明は、前記鍵管理装置であって、前記部分集合に対して割り当てた鍵を前記端末装置に配布する鍵配布部を備え、前記鍵配布部は、鍵を配布する端末装置が含まれる部分集合のうち、最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布し、さらに、前記配布した鍵から生成される鍵が割り当てられた部分集合を除く部分集合から、前記端末装置が含まれる最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布することを特徴とする。

【００２９】

また、本発明は、前記鍵管理装置であって、前記無効化情報生成部は、有効な端末装置だけが含まれる最大の部分集合を選択して、前記選択した部分集合に含まれない端末装置に対しては、さらに、それら端末装置だけが含まれる最大の部分集合を選択して、前記選択を、全ての有効な端末装置が何れかの部分集合に含まれるまで繰り返し行うことを特徴とする。

【００３０】

また、本発明は、記録媒体から無効化情報を読み出して処理する端末装置であって、前記端末装置は、前記無効化情報を処理する鍵を格納する格納部を備え、前記格納部には、自身が含まれる部分集合に割り当てられた鍵を格納することを特徴とする。

また、本発明は、前記端末装置であって、前記格納部は、鍵と部分集合の対応関係を示す情報も合わせて格納することを特徴とする。

【００３１】

また、本発明は、前記端末装置であって、前記格納部は、ある部分集合に割り当てられた鍵から、他の部分集合の鍵が生成可能な場合、前記生成可能な鍵は格納しないことを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置は、前記格納部に格納する鍵か

ら、他の部分集合に割り当てられた鍵を生成する鍵生成部を備え、前記鍵生成部は、部分集合と鍵の対応関係、並びに生成された鍵の相互関係から他の部分集合に割り当てられた鍵を生成することを特徴とする。

【００３２】

また、本発明は、前記端末装置であって、前記端末装置は、前記記録媒体に対して、暗号化されたコンテンツを記録する記録部を備えることを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置は、前記記録媒体から暗号化されたコンテンツを読み出して復号、及び再生する再生部を備えることを特徴とする。

また、本発明は、特定の装置を無効化するための無効化情報を記録する記録媒体であって、鍵管理装置は、著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備え、前記鍵管理装置により生成された無効化情報を記録することを特徴とする。

【００３３】

また、本発明は、前記記録媒体であって、前記鍵管理装置が生成した無効化情報には、どの部分集合の鍵に基づいて生成したのかを示す情報が付与されており、前記付与された情報と共に前記鍵無効化情報を記録することを特徴とする。

【発明の効果】

【００３４】

本発明によれば、各装置が内蔵する鍵の数を削減することが可能である、具体的には、木構造の高さをＴとした場合、当該システムに属する１／２台の装置においてＴ－１個の鍵が削減され、１／４台の装置においてＴ－２個の鍵が削減され、１／（２＾ｋ）台の装置においてＴ－ｋ個の鍵が削減される。

【発明を実施するための最良の形態】

【００３５】

以下、本発明の実施の形態について、図面を用いて説明する。

図１は、本発明における著作権保護システムの概念図を示している。著作権保護システム１は、鍵管理装置１００、記録装置１１０、記録媒体１２０、再生装置１３０からなる。鍵管理装置１００は、記録装置１１０、並びに再生装置１３０に対してデバイス鍵を発行し、デバイス鍵は各装置の内部に格納される。また、鍵管理装置１００は、記録媒体１２０に対して鍵無効化データを発行し、鍵無効化データは記録媒体１２０に記録される。記録装置１１０は、記録媒体１２０が挿入された場合、記録媒体１２０から鍵無効化データを読み出し、デバイス鍵を用いて処理することで、コンテンツの暗号化に利用する鍵を獲得することができる。そして、獲得した鍵に基づいてコンテンツを暗号化して、暗号化コンテンツを記録媒体１２０に記録する。再生装置１３０は、コンテンツが記録された記録媒体１２０が挿入された場合、記録媒体１２０から鍵無効化データを読み出し、デバイス鍵を用いて処理することで、暗号化コンテンツの復号に必要な鍵を獲得することができる。そして、獲得した鍵に基づいて暗号化コンテンツを復号して、コンテンツを再生する。

【００３６】

図２は、鍵管理装置１００の構成要素を示している。鍵管理装置１００は、木構造に対する各装置の割り当て状態、並びにデバイス鍵に関する情報を格納する鍵情報生成／格納部２０１と、鍵情報生成／格納部２０１に格納する情報から、記録装置１１０、並びに再生装置１３０に発行するデバイス鍵を選択して配布するデバイス鍵配布部２０２と、無効化すべき装置を特定する無効化装置特定部２０３と、鍵情報生成／格納部２０１に格納する情報、並びに無効化装置特定部２０３が特定した無効化装置に関する情報から、記録媒体１２０に記録する鍵無効化データを生成する鍵無効化データ生成部２０４を備える。また、鍵情報生成／格納部２０１は、図３に示すような木構造を利用して各装置を管理している。

【００３７】
図３は、２分木の木構造で装置の総数を８台とした場合の例を示している。木構造における各層をレイヤと呼び、レイヤ０のノードをルート、最下位レイヤ（図３の例では、レイヤ３）のノードをリーフと呼ぶ。また、各装置は、木構造のリーフに対して１対１に割り当てられる。
次に、鍵管理装置１００が鍵情報生成／格納部２０１において、デバイス鍵の生成、及び管理を行う方法について説明する。ここでは、その一例として、テーブルを利用して、木構造のリーフに割り当てられた装置の部分集合と、デバイス鍵との対応関係を管理する方法についてその詳細を説明する。テーブルを作成する動作フローを図４に示す。
【００３８】
Ｓ４０１：木構造の高さをＴとする。図３に示す木構造の例では、Ｔ＝３である。
Ｓ４０２：以下のＳ４０３からＳ４０８までの操作をｉ＝０～Ｔまで繰り返し行う。
Ｓ４０３：レイヤｉに存在するノードの数をＮとし、レイヤｉに存在するノードをルートとした部分木の高さをＨとする。図３に示す木構造の例では、ｉ＝１の場合、ノードの数Ｎ＝２、部分木の高さＨ＝２である。
【００３９】
Ｓ４０４：以下のＳ４０５からＳ４０７までの操作をｊ＝０～Ｈ－１まで繰り返し行う。
Ｓ４０５：以下のＳ４０６の操作をｋ＝１～Ｎまで繰り返し行う。
Ｓ４０６：レイヤｉの左からｋ番目のノードをルートとする部分木から、２＾ｊ個の装置だけを除いた装置の部分集合を生成する。そして、生成した部分集合を、テーブルのｊ＋１行目の左から順に格納していく。ただし、複数の装置を除く場合は、除く装置全てが共通の親ノードを持つ場合のみとする。図３に示す木構造の例では、レイヤ０、左から１番目の木構造から２個（ｊ＝１）の端末を除く場合、共通の親ノードを持つ装置１、装置２を除くパターン、同じく共通の親ノードを持つ装置３、装置４を除くパターン、さらに共通の親ノードを持つ装置５、装置６を除くパターン、最後に共通の親ノードを持つ装置７、装置８を除くパターンの４パターンとなり、テーブルの２行目の左から順に格納する。
【００４０】
Ｓ４０７：ｋ＝ｋ＋１を計算してＳ４０５に戻る。
Ｓ４０８：ｊ＝ｊ＋１を計算してＳ４０４に戻る。
Ｓ４０９：ｉ＝ｉ＋１を計算してＳ４０２に戻る。
以上の操作により生成されたテーブルを図５に示す。テーブルの１行目５０１は、木構造全体（装置数８）の集合から、装置を１台だけ除いた場合の部分集合を示している。さらに、テーブルの２行目５０２は、同じく木構造全体の集合から、共通の親を持つ装置２台を除いた場合の部分集合を示し、３行目５０３は、共通の親を持つ装置４台を除いた場合の部分集合を示している。
【００４１】
次に、生成したテーブルの各要素（部分集合）に対して、デバイス鍵を生成して割り当てる動作フローを図６に示す。ただし、デバイス鍵を示すＫｍ、及びＫｍ＋１のｍとｍ＋１は、鍵が割り当てられる毎に１ずつ増加する値とする。
Ｓ６０１：木構造の高さをＴとする。図３に示す木構造の例では、Ｔ＝３である。
Ｓ６０２：以下のＳ６０３からＳ６０８までの操作をｈ＝１～２＾Ｔまで繰り返し行う。
【００４２】
Ｓ６０３：（Ｔ＾２＋Ｔ）／２行、ｈ列の部分集合に対してデバイス鍵Ｋｍを割り当てる。図５に示すテーブルの例では、６行、１列の部分集合１に対して、まずデバイス鍵が割り当てられる。
Ｓ６０４：以下のＳ６０５からＳ６０７までの操作をｉ＝（（Ｔ＾２＋Ｔ）／２）－１～１まで繰り返し行う。

【００４３】
Ｓ６０５：ｉ－１行目で鍵が割り当てられた部分集合の数をＪとする。以下のＳ６０６の操作をｊ＝１～Ｊまで繰り返し行う。
Ｓ６０６：ｉ－１行目の鍵の割り当てられた部分集合Ａｊを基準として、テーブルのｉ行目を左から順に探索していき、部分集合Ａｊを含む部分集合を最大２つまで見つけ、最初の部分集合をＢｊ、次の部分集合をＣｊとする。さらに、部分集合Ａｊに割り当てられたデバイス鍵を擬似乱数生成器の入力として、その出力Ｋｍ、Ｋｍ＋１をそれぞれ部分集合Ｂｊ、Ｃｊのデバイス鍵として割り当てる。
【００４４】
Ｓ６０７：ｊ＝ｊ＋１を計算してＳ６０５に戻る。
Ｓ６０８：ｉ＝ｉ－１を計算してＳ６０４に戻る。
Ｓ６０９：ｈ＝ｈ＋１を計算してＳ６０３に戻る。
以上の操作により生成された、部分集合とデバイス鍵の対応テーブルを図７に示す。これは、１行、１列は、部分集合１２３４５６７に対してデバイス鍵Ｋ８が割り当てられたことを意味し、１行、２列は、部分集合１２３４５６８に対してデバイス鍵Ｋ９が割り当てられたことを意味する。
【００４５】
また、デバイス鍵の相互関係を示すテーブルを図８に示す。これは、部分集合１に割り当てられたデバイス鍵から、擬似乱数生成器を利用して、部分集合１２のデバイス鍵が生成され、さらに、部分集合１２のデバイス鍵から、同じく擬似乱数生成器を利用して部分集合１２３、並びに部分集合１２４の鍵が生成されたこと意味する。図８より、部分集合１に割り当てられたデバイス鍵からは、擬似乱数生成器を利用することで、部分集合１２、１２３、１２４、１２３４、１２３４５６、１２３４７８、１２３４５６７６、１２３４５６８、１２３４５７８、１２３４６７８の全てのデバイス鍵が算出可能であることが分かる。
【００４６】
次に、鍵管理装置１００がデバイス鍵配布部２０２において、鍵情報生成／格納部２０１に格納するテーブルから、デバイス鍵を選択して、各装置に割り当てる動作フローを図９に示す。
Ｓ９０１：デバイス鍵を与える装置の番号をｎとする。
Ｓ９０２：テーブルの（Ｔ＾２＋Ｔ）／２行、１列を起点として、テーブルの左から右、上から下の順でテーブルの全要素を探索する。ここで、テーブルの全要素をＹとする。以下のＳ９０３の操作をｉ＝１～Ｙまで繰り返し行う。図７に示すテーブルの例では、Ｙ＝３４である。
【００４７】
Ｓ９０３：デバイス鍵を与える装置の番号ｎを含む部分集合に割り当てられている（削除されていない）デバイス鍵Ｋｍを当該装置に与える。さらに、当該デバイス鍵から生成することが可能な全てのデバイス鍵をテーブルから削除する。
Ｓ９０４：ｉ＝ｉ＋１を計算してＳ９０２に戻る。
以上の操作により与えられたデバイス鍵と装置の関係を図１０に示す。装置１には、Ｋ１、Ｋ１５、Ｋ２３、Ｋ２７の４つのデバイス鍵が与えられ、装置２には、Ｋ１２、Ｋ２、Ｋ１６、Ｋ２３、Ｋ２８の５つのデバイス鍵が与えられる。各装置に対しては、図１０に示すテーブルの各行（部分集合とデバイス鍵の対応関係）と、図８に示した、デバイス鍵（部分集合）の相互関係を示すテーブルも一緒に与えられる。
【００４８】
次に、鍵管理装置１００が鍵無効化データ生成部２０４において、鍵無効化データを生成する動作について説明する。鍵無効化データ生成部２０４は、無効化装置特定部２０３が特定した装置番号を除く装置のうち、最も多くの装置が共有するデバイス鍵を図７に示すテーブルから選択する。この操作を、無効化すべき装置を除く全ての装置が持つデバイス鍵が選択されるまで繰り返し行う。

【００４９】
図１１は、装置１を無効化する場合の、記録媒体に格納される鍵無効化データを示している。装置１を除く最大の部分集合は２３４５６７８であり、前記部分集合に割り当てられたデバイス鍵Ｋ２８を用いて暗号化した暗号化メディア鍵が格納されている。さらに、暗号化メディア鍵と共に、暗号化に用いたデバイス鍵を特定するための部分集合に関する情報も合わせて格納する。
【００５０】
図１２は、記録装置１１０、並びに記録媒体１２０の構成要素を示している。記録装置１１０は、鍵管理装置１００より発行されたデバイス鍵を格納するデバイス鍵格納部１２０１と、デバイス鍵格納部１２０１に格納するデバイス鍵と、記録媒体１２０に記録された鍵無効化データから復号鍵を選択／生成する復号鍵生成部１２０２と、鍵無効化データを復号鍵生成部１２０２で選択／生成した復号鍵で復号する復号部１２０３と、復号部１２０３で復号して得たメディア鍵でコンテンツ鍵を暗号化する暗号化部１２０４と、コンテンツ鍵でコンテンツを暗号化する暗号化部１２０５を備える。記録媒体１２０は、鍵管理装置１００より発行された鍵無効化データを格納する鍵無効化データ格納部１０１１と、暗号化されたコンテンツ鍵を格納する暗号化コンテンツ鍵格納部１０１２と、暗号化されたコンテンツを格納する暗号化コンテンツ格納部１０１３を備える。
【００５１】
例えば、記録装置１１０が装置３で、Ｋ１３、Ｋ３、Ｋ２４、Ｋ２５の４つのデバイス鍵を持つ場合、記録媒体に記録されている部分集合に関する情報２３４５６７８と、図８に示すデバイス鍵（部分集合）の相互関係を示すテーブルを用いて、デバイス鍵Ｋ２４を選択し、選択したＫ２４と、擬似乱数生成器を１回用いることにより、Ｋ２８を生成してメディア鍵を復号する。
【００５２】
図１３は、記録装置１１０によりコンテンツが記録された記録媒体の例を示している。
図１４は、記録媒体１２０、並びに再生装置１３０の構成要素を示している。なお、記録媒体１２０の構成要素は図１０と同様であるため、その説明は省略する。再生装置１３０は、鍵管理装置１００より発行されたデバイス鍵を格納するデバイス鍵格納部１４０１と、デバイス鍵格納部１４０１に格納するデバイス鍵と、記録媒体１２０に記録された鍵無効化データから復号鍵を選択／生成する復号鍵生成部１４０２と、鍵無効化データを復号鍵生成部１４０２で生成した復号鍵で復号する復号部１４０３と、復号部１４０３で復号して得たメディア鍵で、記録媒体１２０から読み出した暗号化コンテンツ鍵を復号する復号部１４０４と、復号部１４０４で復号して得たコンテンツ鍵で、同じく記録媒体１２０から読み出した暗号化コンテンツを復号する復号部１４０５を備える。
【００５３】
例えば、再生装置１３０が装置７で、Ｋ３０、Ｋ２０、Ｋ７、Ｋ８の４つのデバイス鍵を持つ場合、記録媒体に記録されている部分集合に関する情報２３４５６７８と、図８に示すデバイス鍵（部分集合）の相互関係を示すテーブルを用いて、デバイス鍵Ｋ２０を選択し、選択したＫ２０と、擬似乱数生成器を３回用いることにより、Ｋ２８を生成してメディア鍵を復号する。
【００５４】
（その他の変形例）
（１）本発明では、記録媒体をＤＶＤ－ＲＡＭのようなレコーダブルメディアとする構成としたが、本発明はその構成に限定されるものではない。例えば、記録媒体をＤＶＤ－Ｖｉｄｅｏのようなプリレコーディッドメディアとして、各再生装置がデバイス鍵を保有して、記録媒体に記録されたコンテンツを再生する構成であってもよい。また、この場合、記録媒体への書き込み装置がデバイス鍵を保有する必要はなく、鍵管理装置から直接メディア鍵を受け取り、そのメディア鍵に基づいてコンテンツを暗号化して書き込む構成であってもよい。
【００５５】

（２）本発明では、コンテンツを暗号化するメカニズムとして、メディア鍵でコンテンツ鍵を暗号化して、コンテンツ鍵でコンテンツを暗号化する構成としたが、本発明はその構成に限定されるものではない。例えば、メディア鍵で直接コンテンツを暗号化して鍵階層を１つ減らす構成でもよく、逆にディスク鍵を導入して、メディア鍵でディスク鍵を暗号化して、ディスク鍵でコンテンツ鍵を暗号化して、コンテンツ鍵でコンテンツを暗号化して鍵階層を１つ増やす構成であってもよい。あるいは、鍵階層の途中で別途異なる情報を追加して鍵を変調するような構成であってもよい。

【００５６】

（３）本発明では、鍵無効化データと暗号化コンテンツを同一の記録媒体に記録する構成としたが、本発明はその構成に限定されるものではない。例えば、鍵無効化データを記録する記録媒体と、暗号化コンテンツを記録する記録媒体を変えて配布する構成であってもよい。その場合、記録装置、あるいは再生装置では、まず、鍵無効化データが記録された記録媒体を挿入してメディア鍵を算出してから、別の記録媒体を挿入して、コンテンツの記録、あるいは再生を行う構成となる。

【００５７】

（４）本発明では、鍵無効化データ、並びに暗号化コンテンツを記録媒体に記録して配布する構成としてが、本発明はその構成に限定されるものではない。例えば、放送や、インターネットなどの通信媒体を利用して配布する構成であってもよい。

（５）本発明では、鍵管理装置が、鍵、あるいは各装置を管理するための木構造を２分木として構成したが、本発明はその構成に限定されるものではない。例えば、木構造は３分木であっても、４分木であってもよい。

【産業上の利用可能性】

【００５８】

本発明にかかる鍵無効化システムは、各装置が保持する鍵に対して相互関係を持たせることにより、各装置が持つ鍵の数を削減することができるという効果を有し、同一システムにおいて、据え置き機や携帯端末などが混在する場合に、記憶容量の小さい携帯端末に対しては保持する鍵が少なくなるように割り当てることができるため、鍵無効化を実現するシステムにおいて有用である。

【図面の簡単な説明】

【００５９】

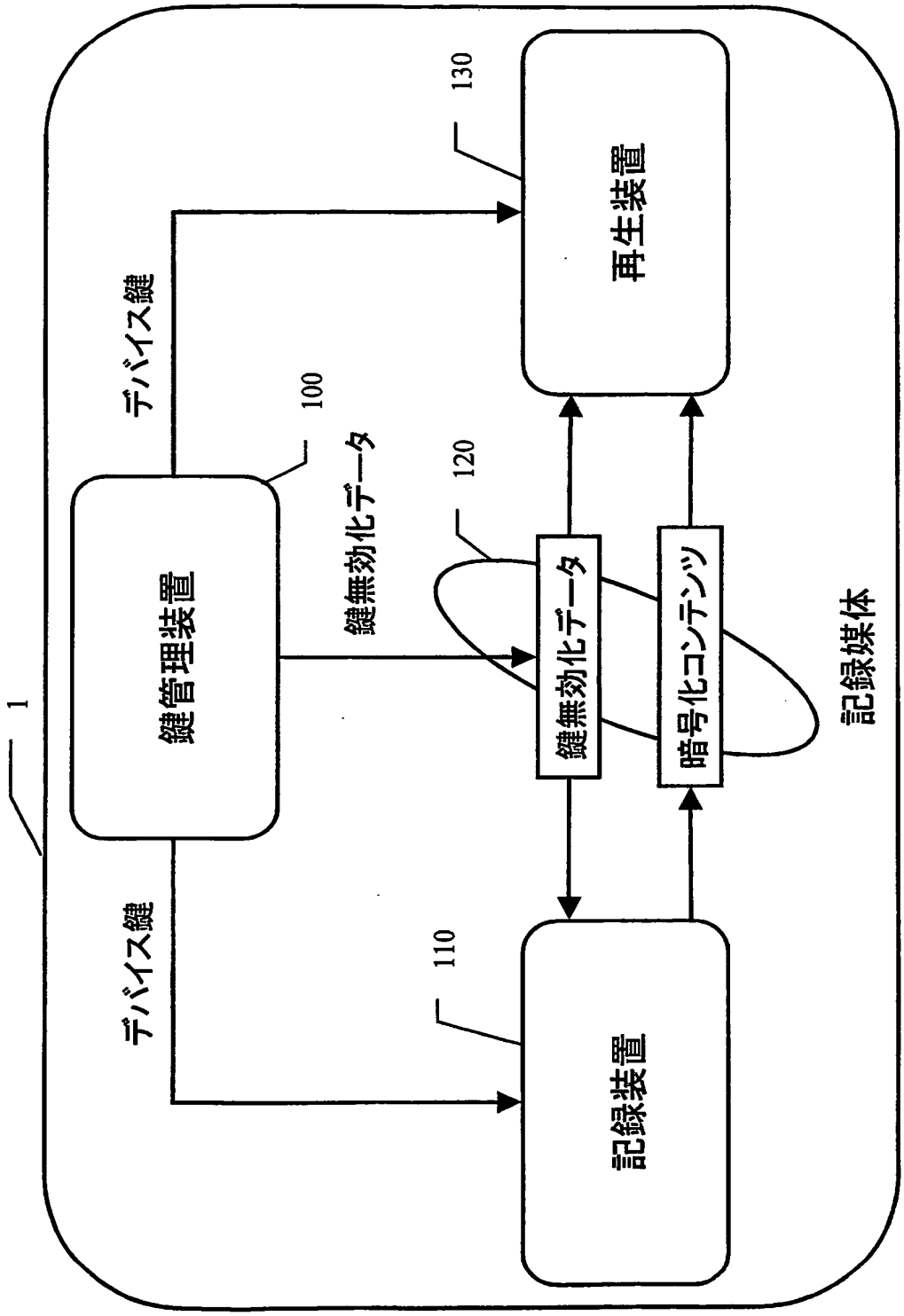
【図１】本発明に係る著作権保護システムの概念図
【図２】本発明に係る鍵管理装置の構成図
【図３】本発明に係る木構造の例を示す図
【図４】本発明に係るテーブル作成の動作フローを示す図
【図５】本発明に係る生成テーブルの例を示す図
【図６】本発明に係るデバイス鍵の割り当ての動作フローを示す図
【図７】本発明に係る生成テーブルの例を示す
【図８】本発明に係るデバイス鍵（部分集合）の相互関係を示す図
【図９】本発明に係る各装置に対するデバイス鍵の割り当ての動作フローを示す図
【図１０】本発明に係る各装置が保持するデバイス鍵の例を示す図
【図１１】本発明に係る記録媒体に格納されるデータの例を示す図
【図１２】本発明に係る記録装置、並びに記録媒体の構成図
【図１３】本発明に係る記録媒体に格納されるデータの例を示す図
【図１４】本発明に係る再生装置、並びに記録媒体の構成図
【図１５】従来技技術の概念図
【図１６】従来技術の木構造の例を示す図
【図１７】従来技術の鍵生成の概念を示す図
【図１８】従来技術の各装置に割り当てるデバイス鍵を示す図

【符号の説明】

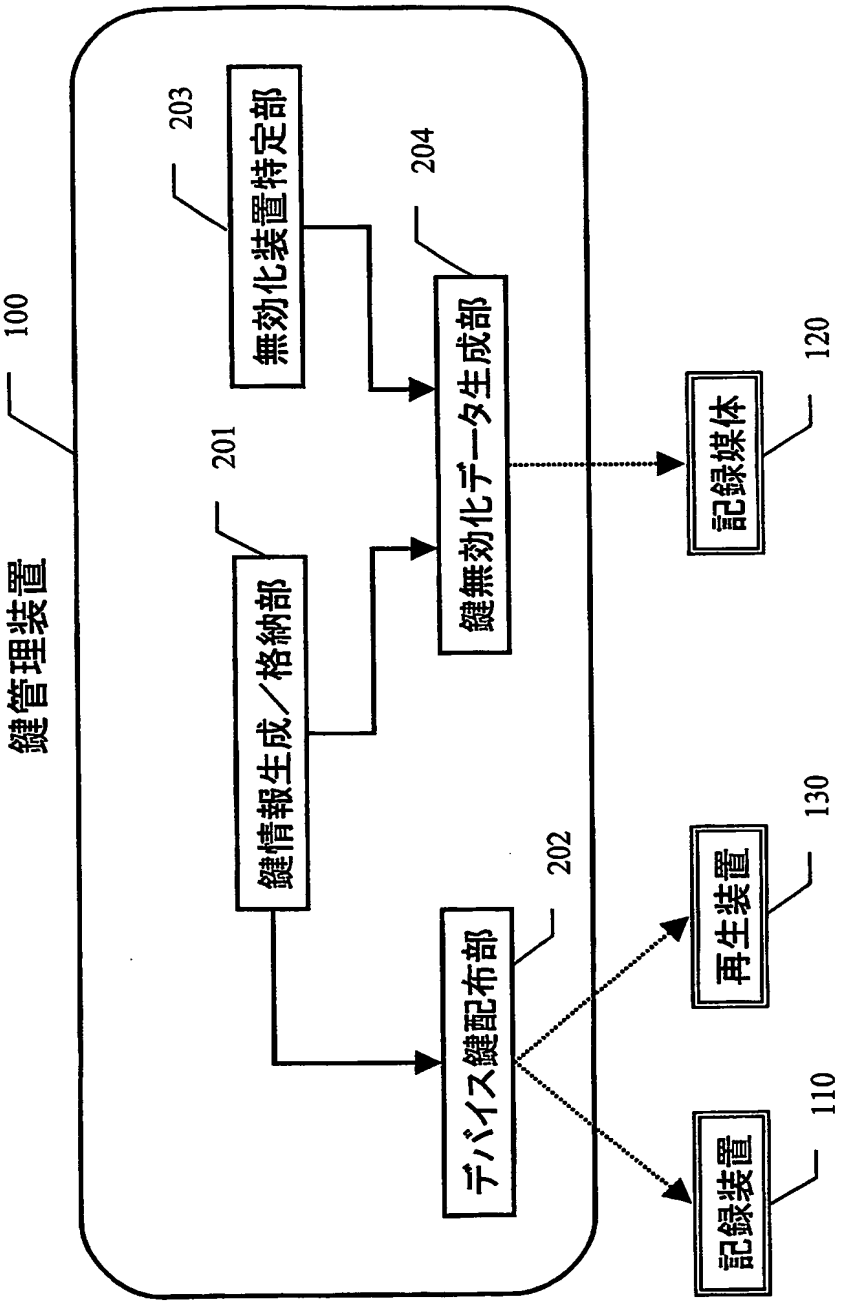
【００６０】

１　著作権保護システム
１００　鍵管理装置
１１０　記録装置
１２０　記録媒体
１３０　再生装置
２０１　鍵情報生成／格納部
２０２　デバイス鍵配布部
２０３　無効化装置特定部
２０４　鍵無効化データ生成部
１０１１　鍵無効化データ格納部
１０１２　暗号化コンテンツ鍵格納部
１０１３　暗号化コンテンツ格納部
１２０１、１４０１　デバイス鍵格納部
１２０２、１４０２　復号鍵生成部
１２０３、１４０３、１４０４、１４０５　復号部
１２０４、１２０５　暗号化部

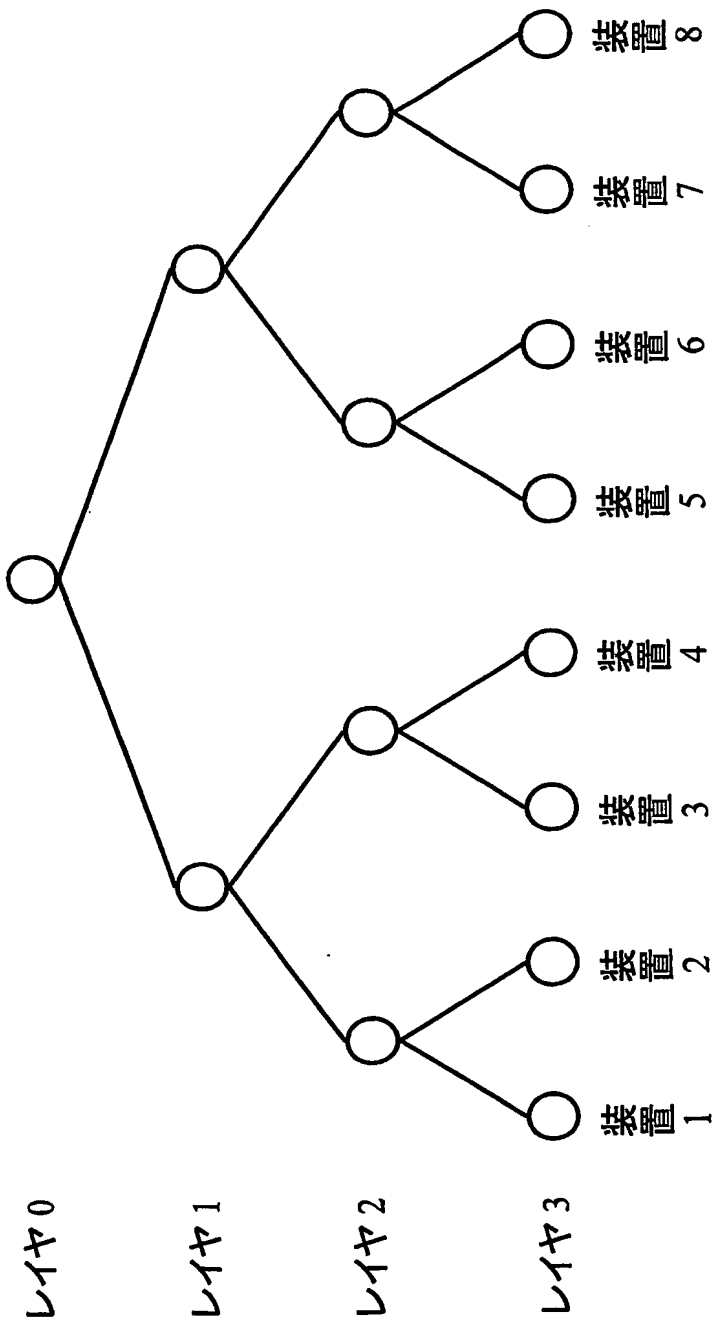
【書類名】図面
【図１】


1
鍵管理装置
100
デバイス鍵
鍵無効化データ
120
130
再生装置
鍵無効化データ
暗号化コンテンツ
記録媒体
デバイス鍵
110
記録装置

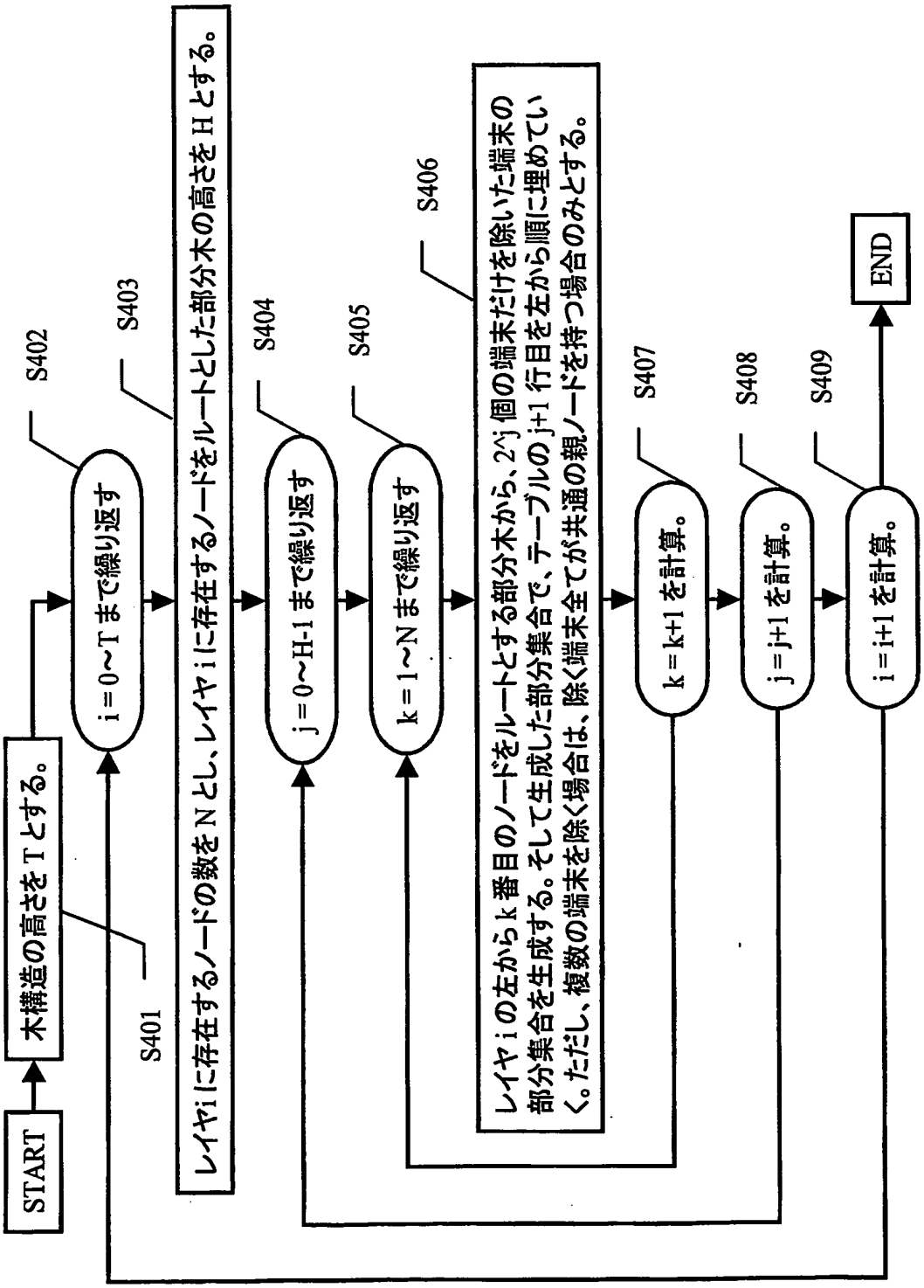
【図２】


鍵管理装置
100
無効化装置特定部
203
鍵情報生成／格納部
201
デバイス鍵配布部
202
鍵無効化データ生成部
204
記録媒体
120
再生装置
130
記録装置
110

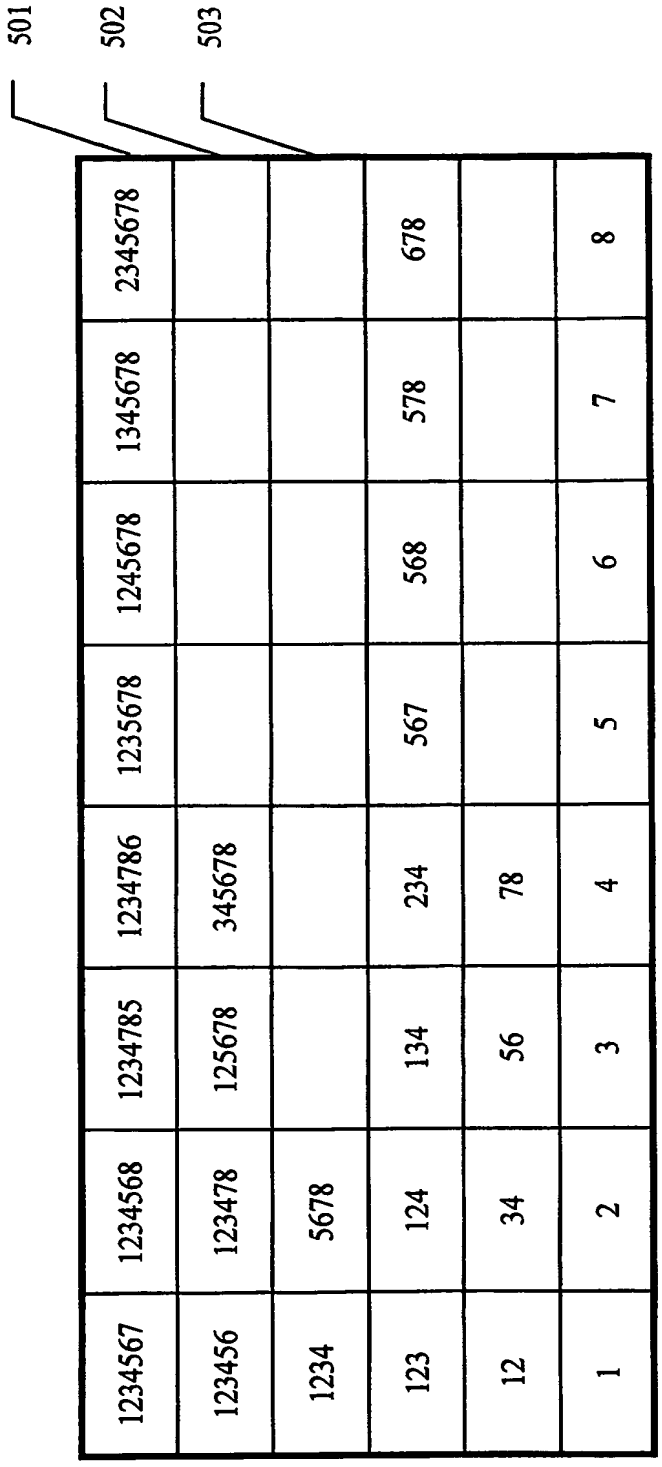
【図３】



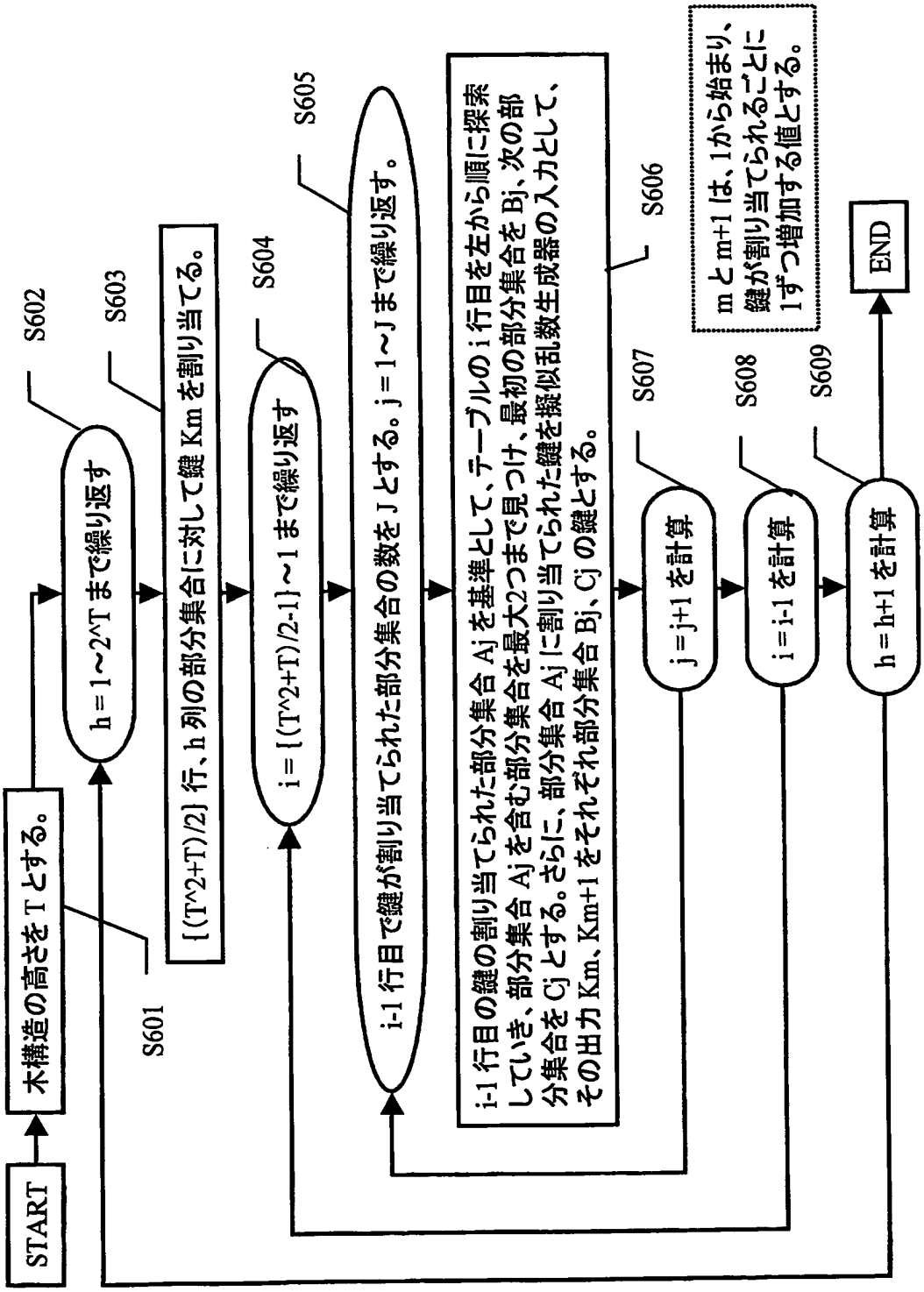
【図４】


START
木構造の高さをＴとする。
S401
S402
i＝0～Ｔまで繰り返す
S403
レイヤiに存在するノードの数をＮとし、レイヤｉに存在するノードをルートとした部分木の高さをＨとする。
S404
j＝0～H-1まで繰り返す
S405
k＝1～Ｎまで繰り返す
S406
レイヤｉの左からｋ番目のノードをルートとする部分木から、2^j 個の端末だけを除いた端末の部分集合を生成する。そして生成した部分集合で、テーブルのj+1 行目を左から順に埋めていく。ただし、複数の端末を除く場合は、除く端末全てが共通の親ノードを持つ場合のみとする。
S407
k＝k+1 を計算。
S408
j＝j+1 を計算。
S409
i＝i+1 を計算。
END

【図５】


501
502
503
1234567
123456
1234
123
12
1
1234568
123478
5678
124
34
2
1234785
125678
134
56
3
1234786
345678
234
78
4
1235678
567
5
1245678
568
6
1345678
578
7
2345678
678
8

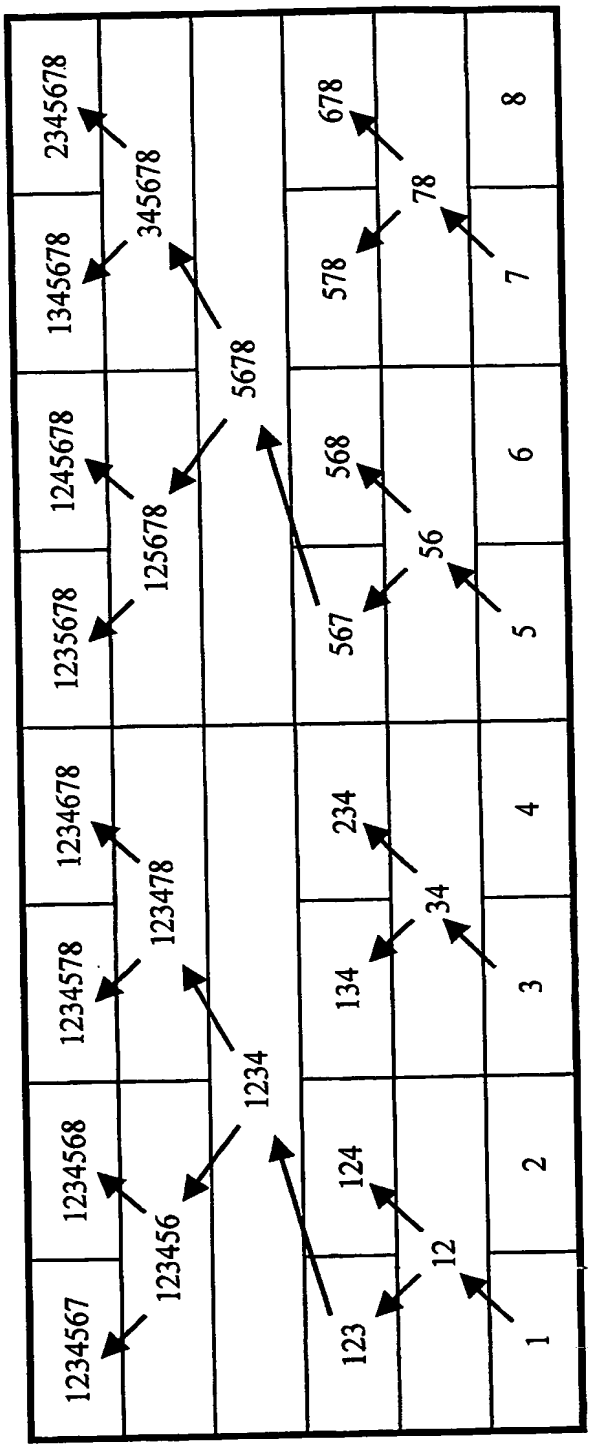
【図６】


START
木構造の高さをTとする。
S601
S602
h＝1～2^Tまで繰り返す
S603
[(T^2+T)/2] 行、h列の部分集合に対して鍵 Km を割り当てる。
S604
i＝{(T^2+T)/2-1}～1まで繰り返す
S605
i-1 行目で鍵が割り当てられた部分集合の数をJとする。j＝1～Jまで繰り返す。
S606
i-1 行目の鍵の割り当てられた部分集合 Aj を基準として、テーブルの i 行目を左から順に探索していき、部分集合 Aj を含む部分集合を最大2つまで見つけ、最初の部分集合を Bj、次の部分集合を Cj とする。さらに、部分集合 Aj に割り当てられた鍵を擬似乱数生成器の入力として、その出力 Km、Km+1 をそれぞれ部分集合 Bj、Cj の鍵とする。
S607
j＝j+1 を計算
S608
i＝i-1 を計算
S609
h＝h+1 を計算
END
m と m+1 は、1から始まり、鍵が割り当てられるごとに1ずつ増加する値とする。

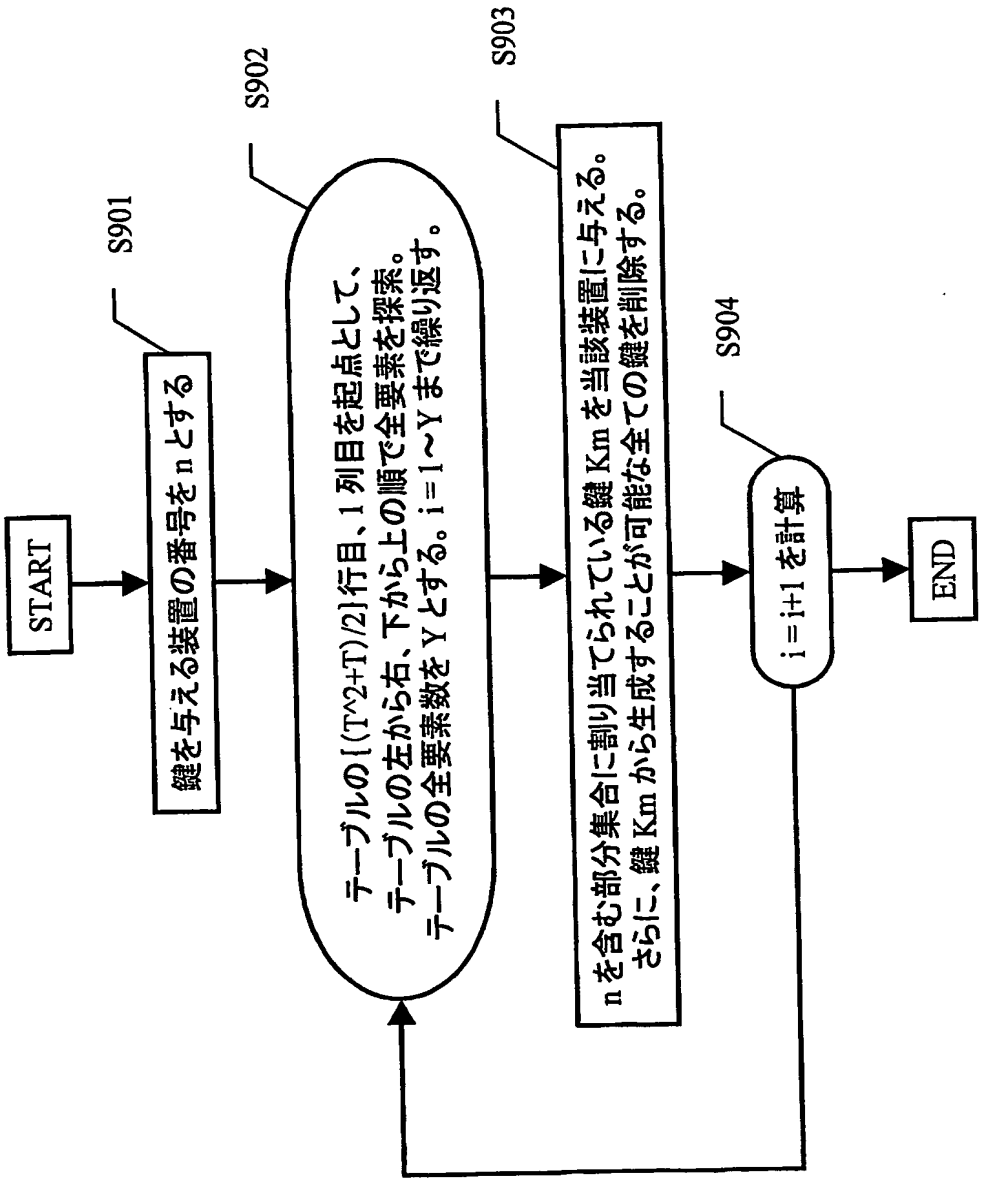
【図７】

1234567 K8	1234568 K9	1234578 K10	1234678 K11	1235678 K25	1245678 K26	1345678 K27	2345678 K28
123456 K6	123478 K7	125678 K23	345678 K24				
1234 K5	5678 K22						
123 K3	124 K4	134 K15	234 K16	567 K20	568 K21	578 K32	678 K33
12 K2	34 K14	56 K19	78 K31				
1 K1	2 K12	3 K13	4 K17	5 K18	6 K29	7 K30	8 K34

【図８】


1234567
123456
1234568
123478
1234578
1234
1234678
123
124
1235678
125678
1245678
12
134
1345678
345678
234
2345678
34
567
5678
568
578
56
78
678
1
2
3
4
5
6
7
8

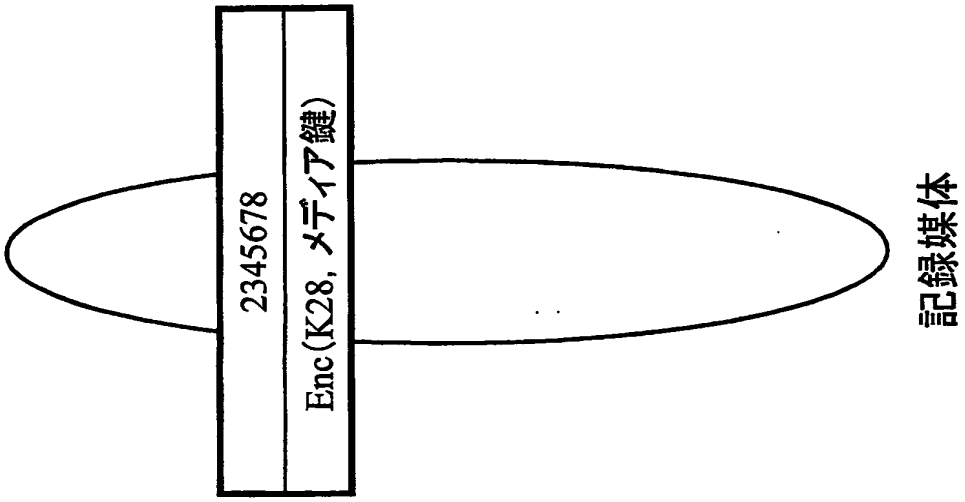
【図９】


START
S901
鍵を与える装置の番号をｎとする
S902
テーブルの{(T^2+T)/2}行目、１列目を起点として、
テーブルの左から右、下から上の順で全要素を探索。
テーブルの全要素数をＹとする。ｉ＝１～Ｙまで繰り返す。
S903
ｎを含む部分集合に割り当てられている鍵Ｋｍを当該装置に与える。
さらに、鍵Ｋｍから生成することが可能な全ての鍵を削除する。
S904
ｉ＝ｉ+1を計算
END

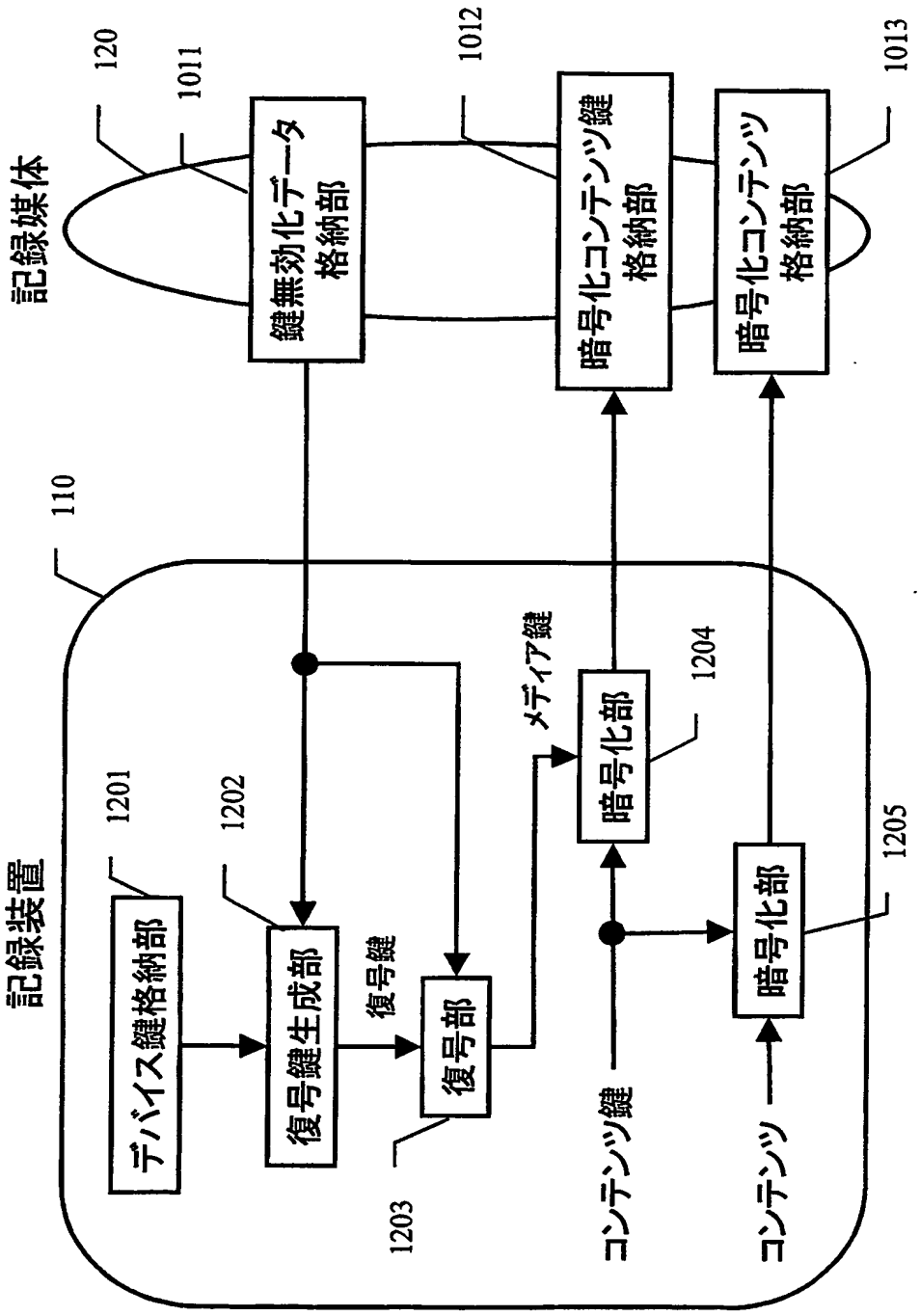
【図１０】

装置1	1 K1	134 K15	125678 K23	1345678 K27		
装置2	2 K12	12 K2	234 K16	125678 K23	2345678 K28	
装置3	3 K13	123 K3	345678 K24	1235678 K25		
装置4	4 K17	34 K14	124 K4	1234 K5	345678 K24	1245678 K26
装置5	5 K18	578 K32	123456 K6	1234578 K10		
装置6	6 K29	56 K19	678 K33	123456 K6	1234678 K33	
装置7	7 K30	567 K20	123478 K7	1234567 K8		
装置8	8 K34	78 K31	568 K21	123478 K7	1234568 K9	5678 K22

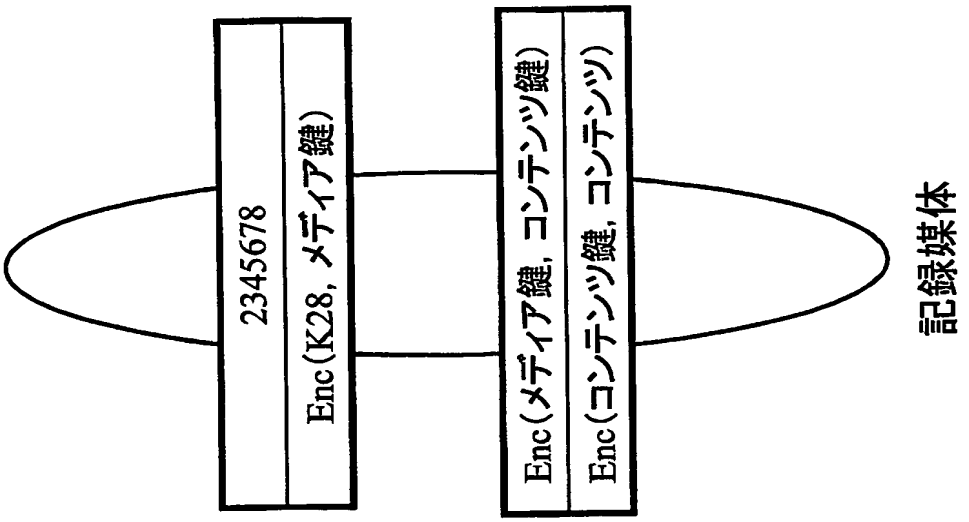
【図１１】



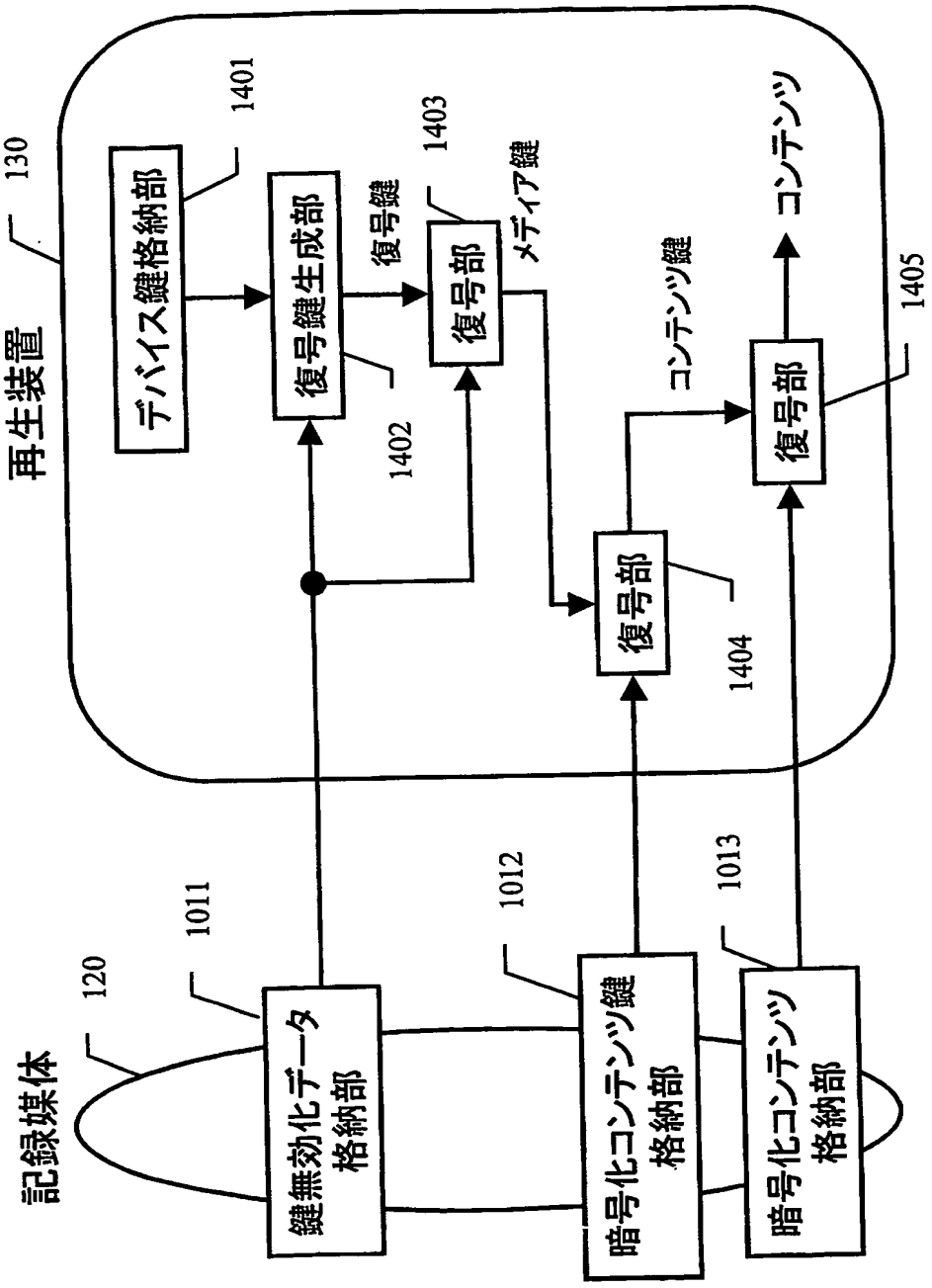
【図１２】


記録媒体
120
1011
鍵無効化データ格納部
1012
暗号化コンテンツ鍵格納部
1013
暗号化コンテンツ格納部
110
記録装置
1201
デバイス鍵格納部
1202
復号鍵生成部
復号鍵
1203
復号部
メディア鍵
1204
暗号化部
コンテンツ鍵
1205
暗号化部
コンテンツ

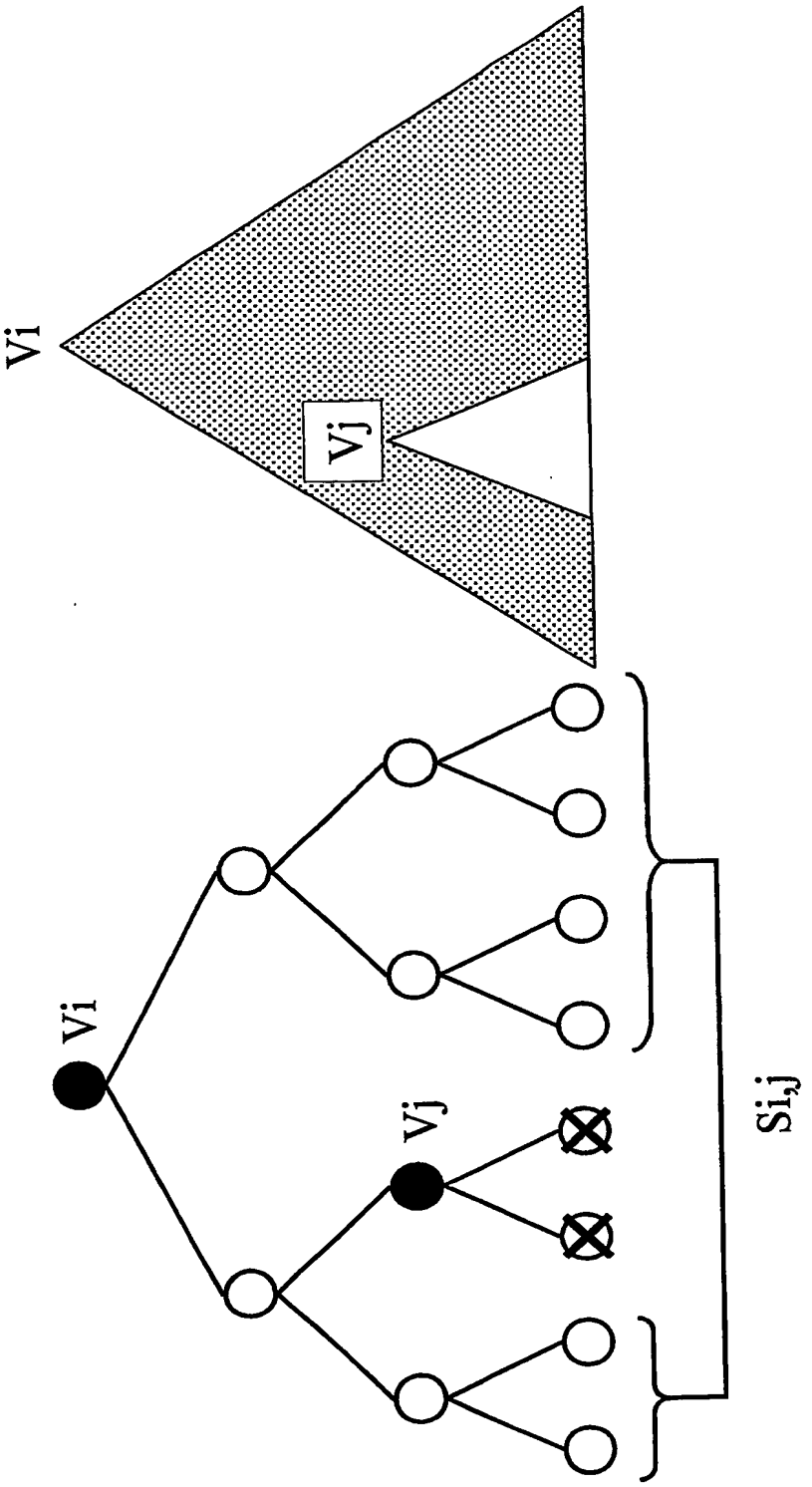
【図１３】


2345678
Enc(K28, メディア鍵)
Enc(メディア鍵, コンテンツ鍵)
Enc(コンテンツ鍵, コンテンツ)
記録媒体

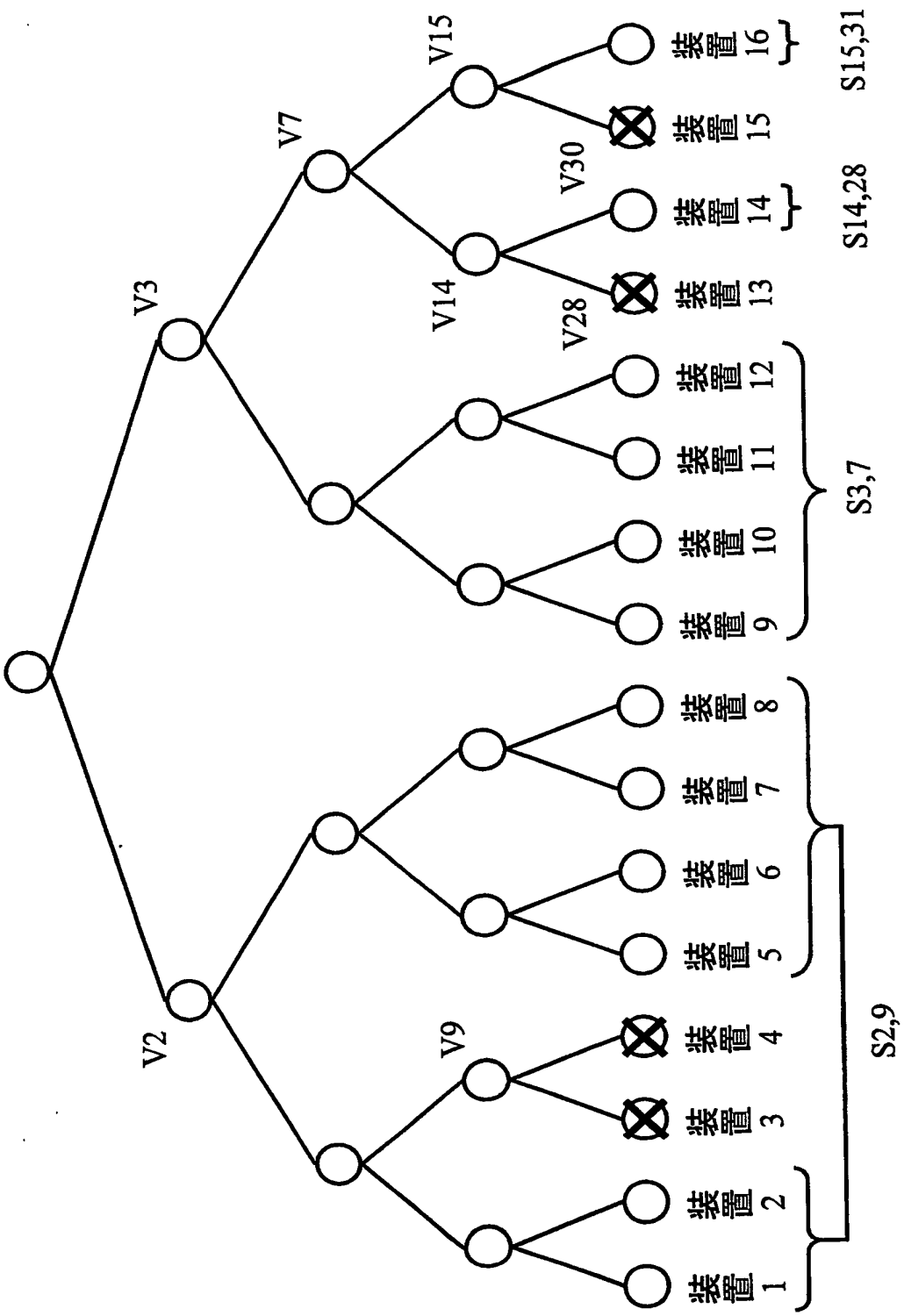
【図１４】


再生装置
130
デバイス鍵格納部
1401
復号鍵生成部
1402
復号鍵
1403
復号部
メディア鍵
復号部
1404
コンテンツ鍵
復号部
1405
コンテンツ
記録媒体
120
鍵無効化データ格納部
1011
暗号化コンテンツ鍵格納部
1012
暗号化コンテンツ格納部
1013

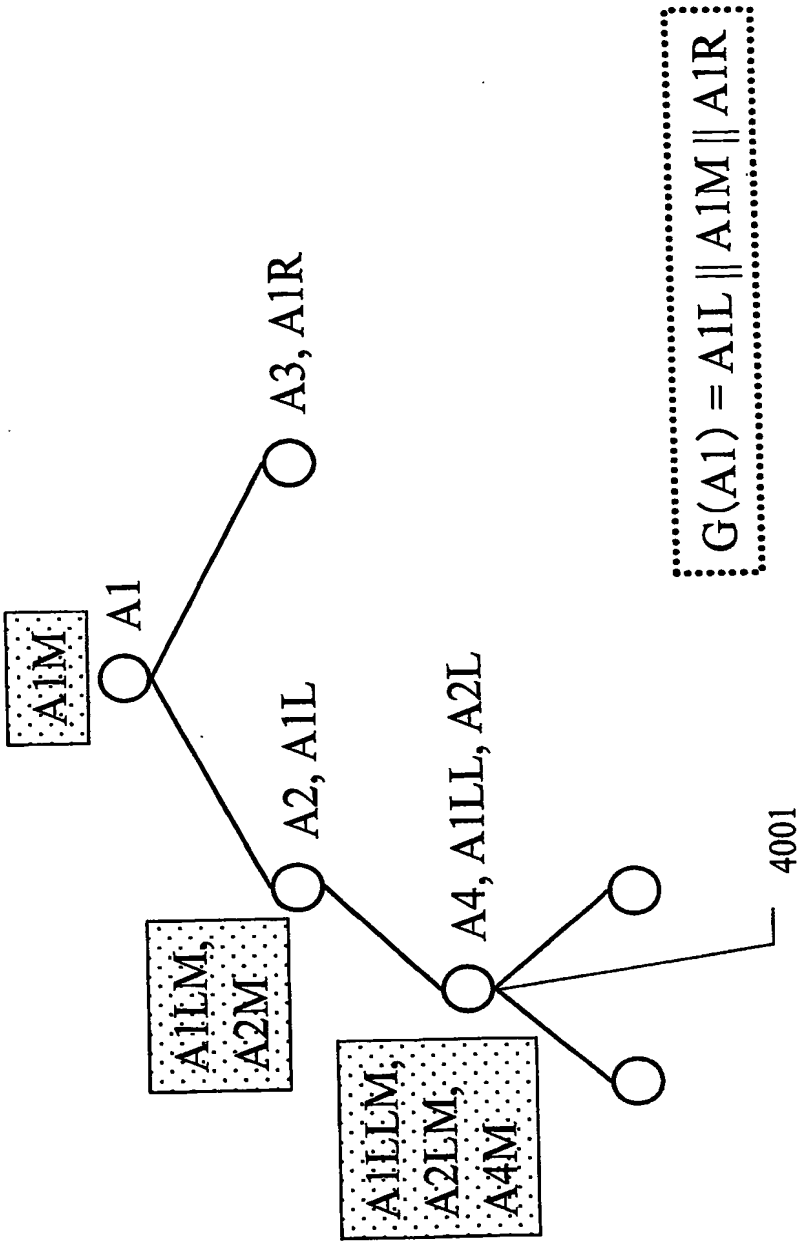
【図１５】



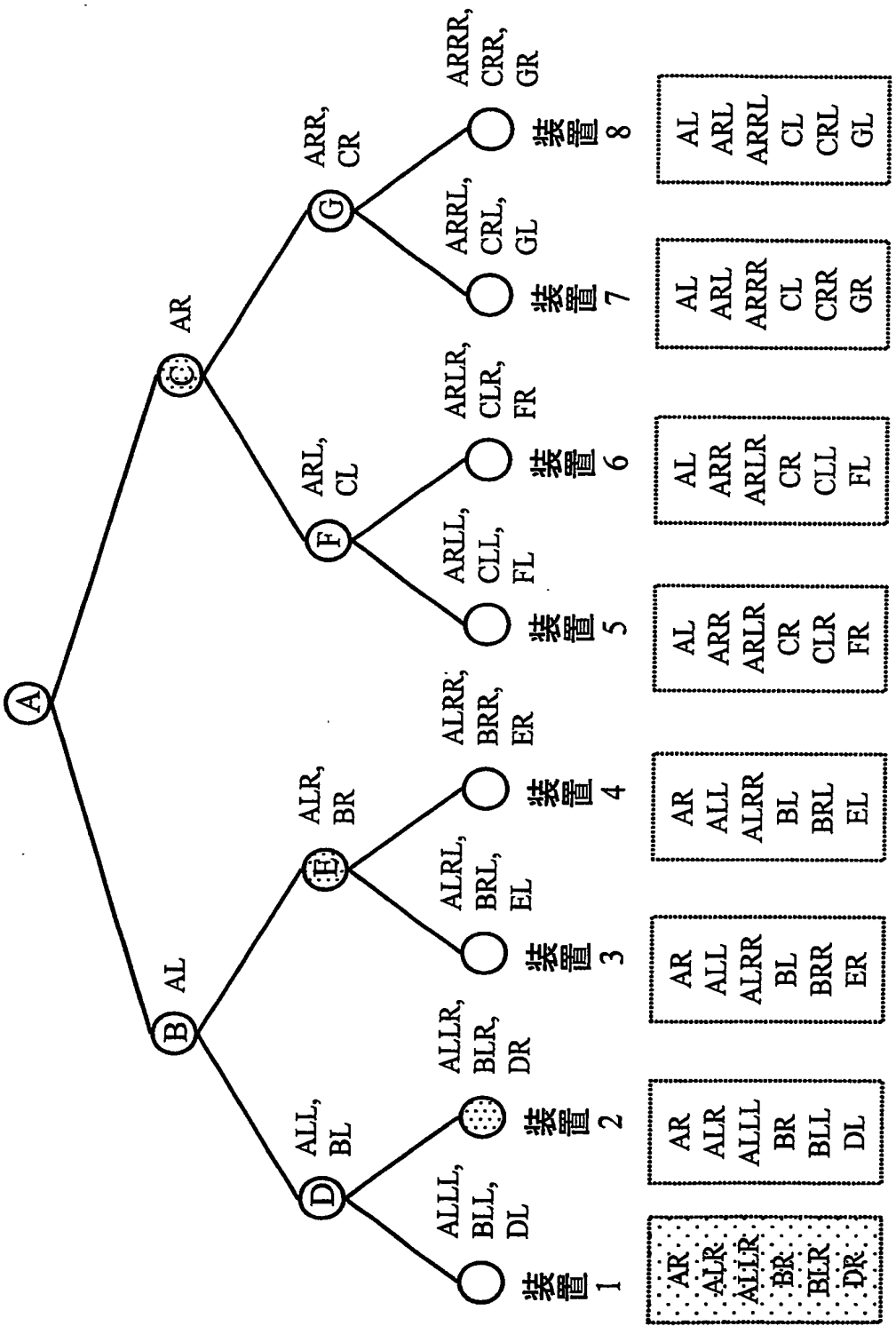
【図１６】


V2
V3
V7
V15
V30
V14
V28
V9
装置 1
装置 2
装置 3
装置 4
装置 5
装置 6
装置 7
装置 8
装置 9
装置 10
装置 11
装置 12
装置 13
装置 14
装置 15
装置 16
S2,9
S3,7
S14,28
S15,31

【図１７】


A1M
A1
A3, A1R
A2, A1L
A1LM,
A2M
A4, A1LL, A2L
A1LLM,
A2LM,
A4M
4001
G(A1) = A1L || A1M || A1R

【図１８】


A
B AL
C AR
D ALL, BL
E ALR, BR
F ARL, CL
G ARR, CR
ALLL, BLL, DL
ALLR, BLR, DR
ALRL, BRL, EL
ALRR, BRR, ER
ARLL, CLL, FL
ARLR, CLR, FR
ARRL, CRL, GL
ARRR, CRR, GR
装置 1
装置 2
装置 3
装置 4
装置 5
装置 6
装置 7
装置 8
AR ALR ALLR BR BLR DR
AR ALR ALLL BR BLL DL
AR ALL ALRR BL BRR ER
AR ALL ALRR BL BRL EL
AL ARR ARLR CR CLR FR
AL ARR ARLR CR CLL FL
AL ARL ARRR CL CRR GR
AL ARL ARRL CL CRL GL

【書類名】要約書
【要約】
【課題】　従来の鍵無効化技術では、各装置が内蔵する鍵の数が膨大となる。
【解決手段】　鍵管理装置は、著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備える。上記構成により、同一システムにおいて、据え置き機や携帯端末などが混在する場合に、記憶容量の小さい携帯端末に対しては保持する鍵が少なくなるように、各装置が保持する鍵に対して相互関係を持たせることにより、各装置が保持する鍵の数を削減する。
【選択図】　図１

特願２００３－３９９９６８

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/017453

International filing date: 25 November 2004 (25.11.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-399968
Filing date: 28 November 2003 (28.11.2003)

Date of receipt at the International Bureau: 27 January 2005 (27.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)